Fairfax County Internal Audit Office

Department of Family Services
Data Classification Audit
Final Report

February 2018

"promoting efficient & effective local government"

Background Information

General

Agencies within Fairfax County Government are responsible for handling sensitive and confidential information during the normal course of operations. County agencies are required to determine data classifications for information processed in County information systems, based on County, legal, and regulatory requirements. Data classifications are used to determine the nature and extent of security and system controls that must be implemented to protect data in information systems. The County Department of Information Technology (DIT) Information Technology Security Policy 70-05.01 defines four pre-determined classes of data. The four classes are confidential, sensitive, internal use and public use. Confidential or sensitive information stored in County information systems includes data such as client or patient health and Social Security Number (SSN) social services and domestic violence information. In addition, several county agencies are required to comply with Health Insurance Portability and Accountability Act (HIPAA) and Virginia codes 63.2-104 and 63.2-104.1 for protection and security of social services and domestic violence information.

Executive Summary

Our audit focused on determining whether policies and procedures were established for classifying agency's data based on the level of sensitivity. Additionally, we focused on determining whether agencies handling sensitive information have controls in place to protect confidential records. Finally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our audit population included three county agencies. A report is being issued for each agency audited.

Department of Family Services (DFS) uses various systems to store and manage electronic records of clients receiving social services and client case management information. We noted that DFS data was identified and classified in accordance with the County Information Security policy and external regulations, user access rights were assigned based on their job responsibilities, disclosure of data was properly authorized and complied with County policies and external regulations. However, we noted the following exceptions where internal controls could be strengthened:

- Forty nine DFS information system users had inappropriate access. We found that user access was not revoked or modified after individuals transferred to other County agencies or after their job responsibilities changed. A summary of systems we noted with improper users are included in the following table:

System/Data base	Total Active Users	Active Users Tested	Improper Active Users Found	Percentage
NNS	34	34	17	50%
SEMS	160	160	11	7%
FCAS	168	15	15	100%
Harmony	383	21	5	24%
Carepath	41	10	1	10%

- The DFS, Office of Woman and Domestic and Sexual Violence Services (OWDSVS) Carepath System had the following access, security and noncompliance issues:

    a) The system vendor user access settings allowed full access to all client information in the system which was not needed.
    b) There was no written agreement with Carepath's vendor for the ownership, security and privacy of County data stored in the Carepath system.
    c) User access granted to OWDSVS enabled staff to change clinical information of clients that they were not servicing.
    d) OWDSVS was accepting and storing in the system client social security number, which was not required for services.

- DFS did not have a formal process to monitor inactive accounts at risk for unauthorized activation by system administrators. We found inactive user accounts in Carepath (124) and FCAS (102) systems, respectively.

Scope and Objectives

This audit was performed as part of our fiscal year 2016 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of July 1, 2016, through June 30, 2017. The objectives of the audit were to determine whether:

- Information systems have been identified and classified in accordance with Information Security Policy 70-05-01 and external regulations.
- There were proper controls over access and changes to confidential and sensitive data.
- Disclosure of confidential and sensitive data was properly protected and authorized.

Methodology

Our audit approach included review of Information Technology Security Policy 70-05.01, to gain an understanding of data classification determination methodology. We reviewed HIPPA regulations to gain understanding of the security rules for information systems processing HIPAA protected health information (PHI). We interviewed department management and staff responsible for data classification policies and procedures, system user access, practices for the disclosure, and protection of sensitive or confidential data. We obtained a list of the systems from DFS and determined the reasonableness of data type classification. We selected a sample of information systems that stored confidential or sensitive information and conducted system walk-throughs to gain an understanding of the data stored in these systems. We performed user access rights test for these sampled systems to ensure user rights are assigned based on their job responsibilities. Lastly, we reviewed disclosure of confidential information or sensitive information for authorization and security. We selected seven systems from DFS for testing. All systems were classified as confidential.

The Fairfax County Internal Audit Office (IAO) is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO reports are available to the public.

Findings, Recommendations, and Management Response

1. Performance of Periodic Review of System User Access

We found that the Department of Family Services (DFS) did not have formal procedures requiring the periodic review of system users to validate the system access by staff. Per our testing we found active user accounts for individuals that no longer needed access for five systems/databases. Summarized below are the systems tested:

.

System/Data base	Total Active Users	Active Users Tested	Improper Active Users Found	Percentage
NNS	34	34	17	50%
SEMS	160	160	11	7%
FCAS	168	15	15	100%
Harmony	383	21	5	24%
Carepath	41	10	1	10%

DFS is required to comply with DIT Security Policy 70-05 01 for system user account administration. DIT Security Policy 70-05 01 Section 3.5.2 *Account Administration* states:

> User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Agency Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications.

Unauthorized users to a system increases the risks of unauthorized disclosure and use of critical or sensitive information. DFS has not established procedures requiring periodic review of user lists to determine user appropriateness. Additionally, there was not process to notify the system administrator of changes to user access.

Recommendation: We recommend that DFS establish procedures requiring the appropriate staff to periodically review all of their system user lists and notify the system administrator when an employee is terminated, transferred or no longer authorized to use the systems. The access for all improper users should be removed. The review should be documented and initialed by the preparer and reviewer.

Management Response: DFS Agency Access Control Administrators(AACA) /security officers conducted an audit of user accounts for the agency's local systems in accordance with Fairfax County Department of Information Technology's Security Policy 70-05 01 Section 3.5.2 *Account Administration.* Access privileges were adjusted when the role or responsibilities of a user had changes, the user no longer needed access to the application or the user was no longer an employee of the department. Access for all improper users was removed in accordance with the concept of least privilege. Completed item December 2017.

Written procedures for the user access review process were completed by the AACA, discussed at an AACA meeting and posted on DFS website. DFS Security Officers will perform future DFS system user access reviews at the same time as the required annual Virginia Department of Social Services system user access reviews. Completed item January 18, 2018

2. Lack of Vendor Access Controls

OWDSVS' Carepath system vendor user account was active and had system administrator access privileges which allowed the vendor full access to the system. It was determined that the vendor didn't need full system access for system maintenance or support functions. Carepath is a web based application. This unmonitored access enabled the vendor to have unauthorized access to client information, increasing the risk of unauthorized disclosure of confidential or sensitive information. OWDSVS was not aware of the level access to Carepath system needed by the vendor for system support and maintenance.

DIT Security Policy 70-05 01 requires that all system users have only the minimum level of access necessary to perform their job responsibilities, and vendor user accounts be activated only when needed for system support and maintenance.

DIT Security Policy 70-05 01, Section 3.5.1 states:

> Data and system owners shall implement operational procedures and technical controls to ensure access to Fairfax County Government information and systems is based upon the principle of least privilege and an authorized need to know and access.

DIT Security Policy 70-05 01, Section 2.8.1 states:

> Third party vendor accounts and maintenance equipment on the Fairfax County network that connects to the Internet, telephone lines, or leased lines shall be disabled when not in use for authorized maintenance or support.

Recommendation: We recommend that the vendor user id be deactivated. When the vendor requires access for maintenance or support, it may be activated after proper authorization. Also, OWDSVS should consult with the vendor to determine the minimum level of access needed by vendor for system maintenance, updates and support. The vendor user ID should be separately managed and the password be updated on agreed upon cycle.

Management Response: OFWDSVS discussed the recommendation to deactivate vendor user id with Carepath. The vendor stated that it is necessary that the vendor account remain active to provide effective and timely system support. OFWDSVS Management Analyst, and DFS Business Analyst for OFWDSVS will ensure minimum level access is used by Carepath, as recommended. Completed item in September 2017.

3. Lack of Vendor Agreement for Carepath System

OWDSVS did not have a written agreement with Carepath's vendor related to ownership, security and privacy of County data stored in the Carepath system. The absence of a written agreement with the vendor for data ownership and protection increases the risks of vendor noncompliance with County, legal, and regulatory data security and privacy requirements; and loss of control over critical agency data if the relationship with the vendor ends.

DIT Security Policy 70-05 01 requires written agreements with system vendors to confirm county ownership of data and vendors' responsibilities for security and protection of county data.

DIT Security Policy 70-05 01 Section 2.8.1 states:

> Third party agreements and contracts shall identify the Fairfax County information to which the third party should have access and state the third party responsibilities in protecting that information.
>
> Agreements and contracts should also define the acceptable methods for the return, destruction, or disposal of Fairfax County information in a third party's possession at the termination of the contract.

Recommendation: OWDSVS should modify the existing agreement with the vendor to include details of each party's responsibilities for data protection and ownership.

Management Response: An existing vendor agreement addresses ownership, security and privacy of County HIPPA data stored in the Carepath system. OFWDSVS and DFS Senior Manager for IT will review and discuss the use of the County's IT Consultant Agreement with Carepath vendor to ensure details of each party's responsibilities for data protection and ownership are covered in the agreement for all OFWDSVS data stored in Carepath. Completed Item on January 31, 2018.

4. Unsuitable System User Access Privileges

We found Carepath users such as OWDSVS administrative staff, counselors and advocates had access to change clinical information of clients for which they were not providing services. While it was necessary for staff to have read access to all client information to prevent record duplication, provide multiple services to a client and perform client intake duties, the ability to edit all client information was not needed. This increased the risks of unauthorized changes to client clinical information. Since all of the staff was required to be available for OWDSVS' intake hotline, OWDSVS' management was concerned that staff would not have client information available in case of a client emergency or crisis, as well as limit the overall service to clients.

The privacy and confidentiality of OWDSVS system data is required by the Virginia law and DIT Security Policy 70-05 01 requires that all system users have only the minimum level of access necessary to perform their job responsibilities.

DIT Security Policy 70-05 01 Section 3.5.1 states: Data and system owners shall implement operational procedures and technical controls to ensure access to Fairfax County Government information and systems is based upon the principle of least privilege and an authorized need to know and access.

Recommendation: We recommend that OWDSVS work with Carepath' s vendor to determine whether Carepath can be configured to allow staff read only instead of edit access to records of clients they are not servicing. This would allow client information to be available to staff, but prevent editing of all client records. For optimal internal controls, when purchasing future case management systems, OWDSVS should assess the cost/benefit of acquiring a system with functionality that allows user edit, data type and specific record access restrictions.

Management Response: OFWDSVS worked with Carepath's vendor to determine the various security levels available in the system, and have established various security roles for users. Admin roles are designated to OFWDSVS Management Analyst and other key personnel. Records management roles are given to supervisory staff. All direct service staff have access only to clients on their respective caseloads and/or assigned to them via their program area or treatment team. Completed item October 1, 2017.

5. Collection and Storage of Social Security Numbers

OWDSVS was accepting and storing client social security numbers that were not required for services in their system. A social security number field was included in an electronic document completed by clients online. During the audit OWDSVS started to delete the stored social security numbers.

The unnecessary collection and storage of social security numbers in an information system increases the risks of client identity theft or unauthorized disclosure of client social security information.

Recommendation: OWDSVS should delete all client social security numbers currently stored in the Carepath system. Also, OWDSVS should modify the electronic form to either remove the social security number field or block data entry into the field. In addition, OWDSVS should develop and implement written procedures requiring employees to immediately delete client social security numbers on online forms.

Management Response: Social Security numbers were removed from active records in Carepath and the Patient Record Information template no longer contains a field requesting an SSN. Completed Item October 1, 2017.

6. Inactive System User Accounts

DFS' Carepath system had 124 of 165 total deactivated user accounts and FCAS system had 102 of 270 total deactivated user accounts that could be easily activated for unauthorized use by the users with system administrator user roles. The Carepath system had 14 users with system administrator roles. There was no evidence to indicate deactivated user accounts were being monitored for unauthorized use.

Unmonitored system deactivated user accounts increases the risk that a current or former staff could use the inactive user IDs to access the system and perform unauthorized activity. DFS did not have a formal process to monitor the accounts nor awareness of the system capabilities to delete the inactive accounts. DFS personnel had been told it may be necessary to retain deactivated user accounts for a period of time to preserve records of user activity.

Recommendation: We recommend that DFS establish a documented process to review deactivated users in the department systems on a regular basis to determine if accounts can be deleted or retained. Consideration should be given to retaining accounts that are needed for operations or to preserve user activity records. The developed process should include timeframes for how long a deactivated account should stay on the system before they are deleted. In addition, procedures for documenting an audit trail for re-activating deactivated accounts should be created and reviewed periodically. Deactivated accounts no longer needed for operations or to preserve user activity records should be deleted from the user ID databases.

Management Response: DFS will review deactivated users in the department systems on a regular basis as part of the agency's documented process for record destruction which is conducted annually. Written procedures are in place for this process and are in accordance with Library of Virginia record retention policy. The deletion of a deactivated user account can only occur if all case records associated with that user account are no longer in the system. When a case record or a user account is purged from the system, the system generates an audit trail of date of deletion. Also, DFS will monitor Carepath system for reactivated accounts. Completed item October 2017.